ABSTRACT

A method for generating cryptographically secure (or unpredictable) pseudo-random numbers uses simple functions whose inverse is not a well-defined function and has a large number of branches, although the inverse could be easily computed on each particular branch. In this way the sequence of numbers is practically unpredictable and at the same time may be generated using very simple functions. A generator of such a pseudo-random bit sequence comprises circuit means for storing bit strings representing integer numbers of the pseudo-random sequence; a shift register coupled to the circuit means; a command circuit generating shift commands for the shift register; second circuit means for storing the bits output by the shift register; an adder modulo 2 summing the bits stored in the second circuit means, generating a bit of the chaos-based pseudo-random bit sequence; a second adder summing up the bit strings currently stored in the shift register and in the first circuit means, generating a bit string representing a successive number of the pseudo-random sequence.